613-001996 Rev.F 150522

Allied Telesis

CentreCOM® x230シリーズ リリースノート

この度は、CentreCOM x230 シリーズをお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書、コマンドリファレンスの補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 5.4.5-0.1

2 本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.4-3.6** から **5.4.5-0.1** へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 Link trap の Private MIB サポート

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

snmp trap link-status コマンドで対象インターフェースのリンクステータスが変化したときに、SNMP のリンクステータス通知メッセージ（プライベート MIB の atLinkUp、atLinkDown トラップ）を生成するようにする enterprise オプションをサポートしました。プライベート MIB の atLinkUp、atLinkDown トラップには、標準 MIB には含まれない、ポートのインターフェース名の情報が含まれています。

2.2 マネージメントスタック

参照 「コマンドリファレンス」/「運用・管理」/「マネージメントスタック」

マネージメントスタック機能をサポートしました。マネージメントスタックは、ネットワーク内に存在する複数のスイッチを、1 台のスイッチから一括して制御するための機能です。

2.3 カッパーケーブル簡易診断

参照 「コマンドリファレンス」/「インターフェース」/「一般設定」

TDR（Time-Domain Reflectometry）方式によるカッパーケーブルの簡易診断ができるようになりました。追加されたコマンドは下記 3 コマンドです。

- ○ clear test cable-diagnostics tdr
- ○ show test cable-diagnostics tdr
- ○ test cable-diagnostics tdr interface

2.4 Web 認証の機能拡張・機能改善

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

- ○ Web 認証サーバーにおいて、HTTPS 標準である 443 番ポート以外への通信を Web 認証サーバーの HTTPS 待ち受けポートにリダイレクトできるようになりました。設定は、新しく追加された auth-web-server ssl intercept-port コマンドで行います。

○ Web 認証サーバーにおいて、HTTP と HTTPS を同時に有効化することができるようになりました。同時有効化の設定は、auth-web-server ssl コマンドに追加された hybrid オプションで行います。

○ Web 認証サーバーの HTTPS リダイレクト機能において、リダイレクト先 URL に含める Web 認証サーバーのホスト名を任意に設定できるようになりました。これにより、独自証明書を利用している環境において、HTTPS リダイレクト機能を経由したアクセス時にも Web ブラウザーの警告が出ないようにすることが可能となります。設定は、新しく追加された auth-web-server host-name コマンドで行います。

○ auth-web-server intercept-port コマンドに any オプションを追加しました。any を指定すると全ポートをプロキシーポートとして監視可能になります。

○ Supplicant と Web 認証サーバーの間で、プロキシー例外の設定ミスによりプロキシー要求のループが発生した際、ループを検出し、Supplicant にエラーページを返すようになりました。

○ ポート認証機能を使用するときの、各ポートへ入力する設定コマンドのテンプレート化が可能になりました。必要な認証関連のコマンドをテンプレートに集約した後、作成したテンプレートを任意のポートに設定します。これにより、複数の認証ポートをより簡単に作成することができます。

2.5 エージングタイムの無効化

参照「コマンドリファレンス」/「L2 スイッチング」/「フォワーディングデータベース」

mac address-table ageing-time コマンドでエージングタイムを無効にする none オプションをサポートしました。

2.6 DHCP クライアント機能

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

DHCP クライアント機能をサポートしました。

3 本バージョンで仕様変更された機能

ファームウェアバージョン **5.4.4-3.6** から **5.4.5-0.1** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 スタティックチャンネルグループの仕様変更

参照「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション (IEEE 802.3ad)」

static-channel-group コマンドで、ポリシーマップをスタティックチャンネルグループの所属ポートに設定する場合に指定する member-filters オプションをサポートしました。

3.2 2 ステップ認証の仕様変更

参照「コマンドリファレンス」/「インターフェース 」/「 ポート認証」

2 ステップ使用時に同一のユーザー名、パスワードを使用すると認証が失敗するようになりました。

3.3 L3 モード エンハンスト ゲスト VLAN の仕様変更

参照「コマンドリファレンス」/「インターフェース 」/「 ポート認証」

インターフェースモードの auth guest-vlan コマンドの routing オプションがなくなり、インターフェースモードの auth guest-vlan forward コマンドを設定することで L3 モード エンハンスト ゲスト VLAN が使用可能になりました。

3.4 atmf working-set コマンドの仕様変更

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク（AMF）」

atmf working-set コマンドで、指定したノードをワーキングセットから削除する no 形式をサポートしました。

4 本バージョンで修正された項目

ファームウェアバージョン **5.4.4-3.6** から **5.4.5-0.1** へのバージョンアップにおいて、以下の項目が修正されました。

4.1 show license コマンドの表示結果で、Base License にサポートしていない、VRRP と RADIUS-100 が表示されていましたが、これを修正しました。

4.2 boot config-file コマンドにおいて、コンフィグファイルを相対パスで指定した場合、show boot コマンドや show system コマンドにおいても相対パスで表示されていましたが、これを修正しました。

4.3 Web 認証、802.1X 認証、ゲスト VLAN を併用したとき、認証成功直後にゲスト VLAN からのエージアウトによって認証が解除される場合がありましたが、これを修正しました。

4.4 glibc に関する脆弱性（CVE-2015-0235）への対策を行いました。

4.5 メール送信機能（mail コマンドやログの出力先の email オプション）を使用して機器からメールを送出する際、SMTP サーバーと正常に通信できない場合、送信に失敗したメールが送信キューに滞留し続けてメモリー容量を消費していましたが、これを修正しました。

4.6 ミラーポートに設定していたポートについて、dot1qVlanStaticTable（1.3.6.1.2.1.17.7.1.4.3）でのポート情報の表示方法を変更しました。

4.7 show ntp associations detail 実行時、XMT の値が正常に表示されないことがありましたが、これを修正しました。また、うるう秒の減算処理に誤りがありましたが、これを修正しました。

4.8 機器が再起動後、NTP マスターとの最初の同期に失敗することがありましたが、これを修正しました。

4.9 OpenSSL 脆弱性（CVE-2014-3569 ～ 3572、CVE-2014-8275、CVE-2015-0204 ～ 0206）への対策を行いました。

4.10 多数の VLAN が所属しているインターフェースを shutdown コマンドでダウンさせた場合に "i/o error on routing socket No buffer space available - disabling" のようなログが出力されることがありましたが、これを修正しました。

4.11 IPv6 アドレスを設定している VLAN を、メンバーポートが存在する状態のまま no vlan で削除すると、関連プロセスが異常終了することがありましたが、これを修正しました。

4.12 ミラーポートに設定されているインターフェースを含む範囲指定で QoS ポリシーマップを設定すると、異常終了する場合がありましたが、これを修正しました。

4.13 LDF パケットに含まれる EtherType、VID、PortID の値が正しくありませんでしたが、これを修正しました。

4.14 認証ポートが MAC 認証、Web 認証を併用しており、かつ直接 Supplicant の Linkup/Down を検知しない環境にて、一度 Web 認証に失敗した後、Supplicant が DHCP の再取得を実施すると、その後 MAC 認証が実施されませんでしたが、これを修正しました。

4.15 802.1X 認証と Web 認証の 2 ステップ認証機能利用時に、ローカル RADIUS サーバーは使用できませんでしたが、これを修正しました。

4.16 auth-mac password コマンドの password 名に「encrypted」を設定することはできませんでしたが、これを修正しました。

4.17 ip route コマンドによる静的経路の設定と auth-web-sever ipaddress コマンドは併用不可でしたが、併用可能になりました。

4.18 Web 認証とゲスト VLAN は併用できませんでしたが、これを修正しました。

4.19 Web 認証サーバーのセッションキープ機能有効時、Web 認証端末が認証画面にアクセスしてから認証に成功するまでの間に、端末上のバックグラウンドプログラム等が自発的な HTTP 通信を試みた場合、認証成功後に意図したページへリダイレクトされないことがありましたが、これを修正しました。

4.20 Web 認証のログインページで、RADIUS サーバーに登録されていないユーザー名とパスワードの組み合わせを入力した際、サプリカントのステータスが正しく表示されませんでしたが、これを修正しました。
また、ログインに成功、または失敗した際に出力されるメッセージも下記に変更されました。
・ {MAC¦801.1X¦Web} Authentication {successful¦ failed} for @() on

4.21 no dot1x port-control で 802.1X 認証を無効化すると、MAC ベース認証、Web 認証の設定も無効になっていましたが、これを修正しました。

4.22 MAC ベース認証を使用しているポートでループによるストームが発生した後、ループを解除した際に Supplicant が接続されている別ポート上で連続的にトラフィックを受信し続けていると、認証解除と認証処理が繰り返されることがありましたが、これを修正しました。

4.23 show power-inline コマンドにおいて、クラス 4 受電機器が接続されたポートの出力上限値の表示が 30000（mW）となるべきところ、15400（mW）として表示されることがありましたが、これを修正しました。

4.24 clear mac address-table コマンドの dynamic オプションでダイナミックエントリーを削除しようとすると関連プロセスが再起動していましたが、これを修正しました。

4.25 マルチキャストパケットを受信中にループが発生し、IGMP Report パケットとマルチキャストの UDP パケットを受信し続けていると nsm プロセスが異常終了することがありましたが、これを修正しました。

4.26 IGMP Snooping が動作しているスイッチ上で、手動によって IGMP グループを削除した場合、Leave メッセージを送信しないことがありましたが、これを修正しました。

4.27 IGMP において、マルチキャストグループに加入している状態で IGMP Snooping を無効にするとハードウェアテーブルにエントリーが残ったままになることがありましたが、これを修正しました。

4.28 AMF 仮想リンクを使用している環境において、仮想リンクが通過する経路上の最小 MTU（経路 MTU）が 1500 バイト未満の場合（例：PPPoE 接続のルーターを介して仮想リンクを設定している場合）、ワーキングセットプロンプトで実行したコマンドの結果が表示されずにプロンプトが返ってくることがありましたが、これを修正しました。

4.29 AMF ネットワークに参加していた AMF ノード (マスターおよび メンバー) が、AMF ポートのリンクダウンなどにより、孤立した場合、そのノードは AMF メンバーの離脱を正しく認識しないことがありましたが、これを修正しました。

4.30 AMF クロスリンクを設定し、マスターからの距離（ホップ数）が同じ機器が 6 台以上存在した状態でトポロジーの変化があると、CPU 使用率の高騰が発生することがありましたが、これを修正しました。

4.31 atmf working-set コマンドにて、複数回連続して任意のグループとローカルノードを行き来すると、各ワーキングセット実行時の内部接続が切断されず、指定したワーキングセットプロンプトに移動できなくなっていましたが、これを修正しました。

4.32 VCS 構成の AMF ノードで VCS のマスター切り替えが発生すると、その後、一部の AMF ノードに接続できなくなることがありましたが、これを修正しました。

4.33 リング構成の AMF ネットワークにおいて、マスターとの接続が断たれた場合、AMF ネットワーク内でループが発生していましたが、これを修正しました。

4.34 AMF マスターのドメインが分割され再構築されたとき、下位ドメインへの downlink のステータスが forwarding に遷移しなくなることがありましたが、これを修正しました。

4.35 atmf virtual-link コマンドで、異なるリモート ID のリンクに同じ IP アドレスを設定できてしまいますが、エラーメッセージが出力されるよう修正しました。

4.36 ワーキングセットを使って AMF メンバーの hostname を変更してしまうと、メンバーが AMF グループから外れていましたが、エラーメッセージを出すよう修正しました。

4.37 AMF メンバーを同時に再起動させると、ワーキングセットで操作できなくなる場合がありましたが、これを修正しました。

4.38 大規模な AMF ネットワークの場合、AMF ノード数に変更があると、show atmf nodes コマンドで表示される Current ATMF node count の値が、機器間で一致しないことがありましたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン **5.4.5-0.1** には、以下の制限事項があります。

5.1 システム

参照 **「コマンドリファレンス」/「運用・管理」/「システム」**

○ システム起動時に下記のコンソールメッセージやログメッセージが出力されることがありますが、動作には影響ありません。

・ コンソールメッセージ
stop: Unable to stop job: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
xx:xx:xx awplus init: getty (ttyS0) main process (XXXX) terminated with status 1

・ ログメッセージ
daemon.warning awplus init: network/getty_console (ttyS0) main process (XXXX) terminated with status 1

○ ドメインリストを設定する場合、最初にトップレベルドメインだけのものを設定すると、同一トップレベルドメインを持つ他のドメインリストを使用しません。その結果、ホスト名を指定した Ping に失敗することがあります。

○ タイムゾーンの設定を変更したとき（clock timezone コマンド実行後）は、設定を保存しシステムを再起動してください。

5.2 コマンドラインインターフェース（CLI）

参照 **「コマンドリファレンス」/「運用・管理」/「コマンドラインインターフェース」**

○ edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。

○ コマンドラインインターフェース（CLI）の操作中に Ctrl/C や Ctrl/Z を入力して反応がなくなった場合は、もう一度 Ctrl/C を入力するか、Ctrl/D を入力してください。

○ enable コマンド（非特権 EXEC モード）のパスワード入力に連続して失敗した場合、エラーメッセージに続いて表示されるプロンプトの先頭に「enable-local 15」という不要な文字列が表示されます。

○ do コマンド入力時、do の後にコマンド以外の文字や記号を入力しないでください。

5.3 ファイル操作

参照「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ ファイル名にスペースは使用できません。

○ フラッシュメモリーから SDHC カードにファイルをコピーするとき、実際にコピーが完了しても、すぐにコピー完了のメッセージが表示されないことがあります。

5.4 ユーザー認証

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

○ TACACS+ サーバーを利用したコマンドアカウンティング（aaa accounting commands）有効時、end コマンドのログは TACACS+ サーバーに送信されません。

○ TACACS+ サーバーを利用した CLI ログインのアカウンティングにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。

○ スクリプトで実行されたコマンドは TACACS+ サーバーへは送信されません。

5.5 RADIUS サーバー

参照「コマンドリファレンス」/「運用・管理」/「RADIUS サーバー」

○ server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとすると、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。

○ ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。

○ サポートリミット以上のユーザー情報が記載されている CSV ファイルを読み込んだとき、ローカル RADIUS サーバーには 1 件も登録されないにも関わらず、「Successful operation」と表示されます。

5.6 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。

○ 複数の VLAN に所属する SFP モジュールをホットスワップすると、次のようなログが表示されます。

user.warning awplus NSM[XXXX]: 601 log messages were dropped - exceeded the log rate limit

これは短時間に大量のログメッセージが生成されたため一部のログ出力を抑制したことを示すものです。ログを抑制せずに出力させたい場合は、log-rate-limit nsm コマンドで単位時間あたりのログ出力上限設定を変更してください。

5.7 スクリプト

参照「コマンドリファレンス」/「運用・管理」/「スクリプト」

間違ったコマンドを入力したスクリプトファイルを実行した場合、本来ならば、コンソール上に "% Invalid input detected at '^' marker." のエラーメッセージが出力されるべきですが、エラーメッセージが出力されないため、スクリプトファイルが正常に終了したかのように見えてしまいますが、通信には影響はありません。

5.8 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

○ トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：
% Script /flash/script-3.scp does not exist. Please ensure it is created before

正：
% Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

○ 定時トリガー（type time）を連続で使用する場合は 1 分以上の間隔をあけてください。連続で実行すると show trigger counter で表示される Trigger activations のカウンターが正しくカウントされません。

5.9 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ snmp-server enable trap コマンドは、省略せずに入力してください。省略した場合、実行できない、または、コンソールの表示が乱れることがあります。

○ IP-MIB は未サポートです。

○ VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。

○ snmp-server enable trap コマンドにおいて、snmp-server の文字列を省略し、sn enable trap と入力すると、入力したコマンドがホスト名欄に表示され、コマンドは認識されません。コマンドは tab 補完などを利用し省略せずに入力してください。

5.10 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

sflow collector コマンドで UDP ポートを変更したのち、UDP ポートを初期値に戻す場合は、「no sflow collector」ではなく「sflow collector port 6343」を実行してください。

5.11 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。

Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。

○ ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル（Stratum）は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

5.12 端末設定

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

仮想端末ポート（Telnet/SSH クライアントが接続する仮想的な通信ポート）がすべて使用されているとき、write memory など一部のコマンドが実行できなくなります。

5.13 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。

- No entry for terminal type "network";
- using vt100 terminal settings.

5.14 Secure Shell

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

○ SSH サーバーにおけるセッションタイムアウト（アイドル時タイムアウト）は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。

○ 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続（コマンド実行）をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。

```
clientHost> ssh manager@192.168.10.1 "show system"
```

○ SSH ログイン時、ログアウトするときに以下のログが表示されますが、動作に影響はありません。

- 23:50:43 awplus sshd[2592]: error: Received disconnect from 192.168.1.2: disconnected by server request

○ manager 以外のユーザー名でログインする際、SSH 接続に RSA 公開鍵を使用した場合であってもパスワードが要求されますので、ユーザー名に紐付くパスワードを入力してください。

○ AlliedWare 製品から AlliedWare Plus 製品への SSH 接続は未サポートです。

5.15 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ SFP ポートでは、polarity コマンドでのインターフェースの極性の固定設定は未サポートです。

○ SFP ポートで Copper SFP（AT-MG8T）を使用する際、Polarity Auto でリンクアップしたときの表示が必ず MDI と表示されてしまいます。

5.16 ポートミラーリング

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ 複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

○ ミラーポートとして設定されたポートは、どの VLAN にも属していない状態となりますが、mirror interface none で、ポートのミラー設定を解除し VLAN に所属させても dot1qVlanStaticTable（1.3.6.1.2.1.17.7.1.4.3 ） にポート情報が当該 VLAN に表示されません。ポートに mirror interface コマンドでソースポートのインターフェースとトラフィックの向きを設定した後、設定を外すとポート情報が正しく表示されるようになります。

5.17 ループガード

参照「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ LDF 送信間隔（loop-protection コマンドの ldf-interval パラメーター）を 1 秒に設定する場合、ループ検出時の動作持続時間（loop-protection timeout コマンド）は 2 秒以上に設定してください（初期値は 7 秒）。

○ LDF 検出機能のアクションが vlan-disable となっている VLAN の所属ポートで、switchport enable vlan コマンドを実行しないでください。

○ MAC アドレススラッシングの検出を SNMP トラップで通知する際、MAC アドレススラッシングプロテクションによるアクションの実施を知らせるトラップが、MAC アドレススラッシングの検出を知らせるトラップよりもわずかに先に送信されることがあります。この現象はトラップでのみ発生し、show log の表示では入れ替わることはないため、実際の順番はログを確認してください。

○ LDF 検出と QoS ストームプロテクションを併用する場合、両方の検出時の動作に port-disable を選択しないでください。どちらか片方は、異なる動作を選択してください。

○ LDF 検出機能でループを検知し、検出時の動作が行われているとき、当該ポートが所属する VLAN を変更しないでください。VLAN を変更した場合、検出時の動作に問題はありませんが、show loop-protection コマンドによる表示が旧 VLAN と新 VLAN の両方表示されます。

5.18 リンクアグリゲーション

参照 「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○ スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。
この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○ スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○ show interface コマンドで表示される poX インターフェース（LACP チャンネルグループ）の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。
LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

○ リンクアグリゲーションを設定した状態で、[no] mac address-table acquire コマンドを実行すると、不要なログメッセージが出力されますが、MAC アドレステーブルの自動学習機能には影響ありません。

○ トランクグループ（saX、poX）を無効化（shutdown）した状態でメンバーポートを削除しないでください。

5.19 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。

○ 認証済みポートが認証を解除されても、マルチキャストトラフィックが該当ポートに転送され続ける場合があります。

○ インターフェース上で、dot1x port-control コマンドを設定する前に dot1x control-direction コマンドを設定しないでください。設定すると「no dot1x control-direction」を実行しても、dot1x control-direction コマンドを削除することができなくなります。その場合は、「no dot1x port-control」を実行してください。

○ auth-web method コマンドで認証方式を変更した場合は、対象ポートをいったんリンクダウンさせ、その後リンクアップさせてください。

5.20 Power over Ethernet

参照 「コマンドリファレンス」/「インターフェース」/「Power over Ethernet」

○ power-inline enable コマンドを no 形式で実行し、PoE 給電機能を無効に設定すると、本来、show power-inline コマンドの Oper の表示が「Disabled」と表示されるべきですが、受電機器が接続されたポートでは「Off」と表示されます。

○ PoE 電源の電力使用量が最大供給電力を上回った場合、show power-inline interface detail コマンドの Detection Status は「Denied」と表示されるべきですが、「Off」と表示されてしまいます。
同様に、ポートの出力電力が上限値を上回った場合、「Fault」と表示されるべきですが、「Off」と表示されてしまいます。

○ ポートの出力電力が上限値を上回った状態で数分間放置すると、実際に接続している受電機器の電力クラスと異なる電力クラスが表示される、または「n/a」と表示されることがあります。また、これに伴って Max も実際とは異なる値が表示されます。ポートの出力電力が上限値未満に戻ると、表示も回復します。

○ ポートの出力電力が上限値を上回った状態のとき、show power-inline の Oper の表示が、実際の「Fault（ポートの出力電力が上限値を上回ったために給電を停止している）」ではなく「Denied（PoE 電源の電力使用量が最大供給電力を上回ったために給電を停止している）」となることがあります。

○ 給電中のポートの PoE 給電機能を無効化しないでください。

○ PoE+ が有効なポートで PoE+ とそれより電力の低いクラスの PoE の信号を短時間に受信した場合、PoE+ 準拠の電力を供給してしまいます。

○ power-inline max コマンドで受電機器の消費電力を下回る値を設定しないでください。また、給電機器で設定している値を超えた電力要求がくると繰り返しトラップを出してしまいますが、通信に影響はありません。

○ インターフェースで PoE 機能を無効にし、再度機能を有効にしたい場合は、5 秒程度経ったあとに行ってください。

5.21 バーチャル LAN

参照「コマンドリファレンス」/「インターフェース」/「バーチャル LAN」

○ プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN ともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN とプライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。

○ エンハンストプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。

○ プライベート VLAN 設定時に一度設定したホストポートは、その後設定を削除しても、show vlan private-vlan の表示に反映されず、ホストポートとして表示されたままになります。

○ プライベート VLAN でセカンダリー VLAN を削除したとき、private-vlan association コマンドの設定を削除することができなくなります。セカンダリー VLAN を削除する場合は、事前に private-vlan association コマンドの設定を削除してください。

○ タグ付きのトランクポートにポート認証が設定されている際、認証の設定を維持したままポートトランキングの設定を削除し、ネイティブ VLAN の設定を行う場合は、一度タ

グなし VLAN に設定を変更してから再度ポートトランキングを設定し、ネイティブ VLAN の設定変更を行ってください。

○ マルチプル VLAN（プライベート VLAN）を CLI から設定した場合、コマンドの入力順序によってはプロミスキャスポート・ホストポート間の通信ができなくなる場合があります。その場合は、設定を保存してから再起動してください。

○ 1 ポートに適用する VLAN クラシファイアグループは 2 グループまでにしてください。

○ 同じ VLAN クラシファイアグループ内に複数のルールを定義した場合、設定順ではなく番号順に反映されます。

○ IP サブネット VLAN が正しく動作せず、パケットが正しい VLAN に転送されません。

○ インターフェースにプライベート VLAN の設定をしたままプライベート VLAN を削除することはできません。プライベート VLAN を削除する場合は次の手順で VLAN を削除するようにしてください。

1. インターフェースに対して switchport mode private-vlan コマンドを no 形式で実行して VLAN の設定を解除する。
2. private-vlan コマンドを no 形式で実行してプライベート VLAN を削除する。

5.22 UDLD

参照「コマンドリファレンス」/「L2 スイッチング」/「UDLD」

UDLD が Unidirectional を検出した場合、show interface コマンドの administrative state 欄には err-disabled と表示されますが、このとき標準 MIB の ifAdminStatus は UP を示します。

5.23 イーサネットリングプロテクション（EPSR）

参照「コマンドリファレンス」/「L2 スイッチング」/「イーサネットリングプロテクション」

○ EPSR 内のリンクダウンが発生した機器が、マスターからのリンクダウンパケットを受け取っても FDB 情報をクリアしない場合があります。また、リンクダウンが発生した機器は本来であれば FDB の全クリアする必要がありますが、該当ポートの FDB はリンクダウンによってクリアされるため、通信に影響はありません。

○ EPSR スーパーループプリベンション構成において、優先順位の低いリングの一部が切れている状態かつ、Common Link が切れている状態で、その Common Link を持つ機器が、再起動をすると、優先順位の低いリングへの接続ポートがリンクアップしているにも関わらず、ポートのステータスがブロッキングになっているため、通信ができません。正しく配線されていることを確認してから起動するようにしてください。

5.24 IP インターフェース

参照「コマンドリファレンス」/「IP ルーティング」/「IP インターフェース」

○ DHCP クライアント機能によって IP アドレスを取得したとき、IP アドレス使用状況確認パケットを送出しません。

○ DHCP クライアント機能を有効に設定できる VLAN インターフェースの最大数は 2000 となります。

5.25 ARP

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

○ マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。

○ 同一 MAC アドレスに対して複数の ARP エントリー（異なる IP アドレス）を登録している場合、そのうちの 1 つを削除すると、残りの ARP エントリーに対応する FDB エントリーも削除されます。その場合は、手動でスタティックな FDB エントリーを登録してください。

5.26 IPv6

参照「コマンドリファレンス」/「IPv6」

○ 自身の IPv6 アドレス宛てに ping を実行するとエラーメッセージが表示されます。

○ フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

5.27 IGMP Snooping

参照「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

○ マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。
IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。

○ ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp

snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。

○ 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。

○ 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されてしまいます。

○ IGMP Snooping 利用時、IGMP Querier を挟まないネットワーク上にマルチキャストサーバーとホストがいる場合、ホストが離脱した後もタイムアウトするまでパケットが転送され続けます。clear ip igmp コマンドで手動でエントリーを削除してください。

5.28 MLD Snooping

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

○ clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。

○ MLD メッセージを受信する環境では MLD Snooping を有効にしてください。MLD snooping が無効に設定されたインターフェースで MLD メッセージを受信すると次のようなログが出力されます。

NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface port6.0.49

○ clear ipv6 mld group * ですべてのグループを削除した場合、ルーターポートのエントリーも削除されてしまいます。
clear ipv6 mld group ff1e::1 のように特定のグループを指定した場合は削除されないため、グループを指定し削除してください。また、削除されてしまった場合も MLD Query を受信すれば再登録されます。

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

○ MLD Snooping を無効にしても一部の MLD Snooping の機能が動作し続けます。このため、show コマンド上の MLD エントリーが更新されつづけたり、MLD のパケットを受信した際に MLD が動作していることを示すログが出力されます。

○ MLD Snooping を一時的に無効にして再度有効にする場合は、無効にしてから有効にするまでに約 5 分間隔を空けてください。

5.29 アクセスリスト

参照「コマンドリファレンス」/「トラフィック制御」/「アクセスリスト」

ARP や IGMP など CPU で処理されるパケットに対してイングレスフィルターが正しく動作しません。
ARP に関しては、以下の設定でフィルターすることが可能です。

```
mls qos enable
access-list 4000 deny any any vlan 100
class-map class1
match access-group 4000
policy-map policy1
class default
class class1
interface port2.0.24
service-policy input policy1
```

5.30 ハードウェアパケットフィルター

参照「コマンドリファレンス」/「トラフィック制御」/「ハードウェアパケットフィルター」

VCS のマスター切り替え後に、既存のハードウェアパケットフィルターへ新規フィルター条件を追加した場合、シーケンス番号が正しく割り振られません。追加処理は正常にできているため、show access-list コマンドの表示順にフィルタリングは機能します。

5.31 Quality of Service

参照「コマンドリファレンス」/「トラフィック制御」/「Quality of Service」

○ match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。no match ip-dscp コマンドを入力することで、設定を削除できます。

○ wrr-queue disable queue コマンドを設定している状態で no mls qos コマンドにより QoS 自体を無効にする場合は、先に no wrr-queue disable queue コマンドを実行してください。

○ QoS の送信スケジューリング方式（PQ、WRR）が混在するポートを手動設定のトランクグループ（スタティックチャンネルグループ）に設定した場合、ポート間の送信スケジュールが正しく同期されません。トランクグループを設定した場合は、個々のポートに同じ送信スケジュール方式を設定しなおしてください。

○ ポリシーマップ名に「|」（縦棒）を使用しないでください。

○ 受信レート検出（QoS ストームプロテクション）機能の storm-action コマンドの初期値に portdisable が設定されています。

○ QoS ストームプロテクションの linkdown アクションを解除するときは、switchport enable vlan コマンドではなく「no shutdown」を使ってください。

○ mls qos enable コマンドを no 形式で実行しても、一部の mls qos 関連のコマンドがランニングコンフィグから削除されないことがあります。不要な場合は no 形式で実行して削除してください。

5.32 アライドテレシスマネージメントフレームワーク（AMF）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

○ AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたがってください。

[手順 A]

1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]

1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
2. 設定や構成を変更する。
3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。

○ リブートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。

○ AMF マスターが AMF メンバーよりも後から AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で atmf restricted-login コマンドを実行することで、すべての AMF メンバーに対して制限をかけることができます。

○ AMF クロスリンクを抜き差しすると、show atmf links statistics コマンドの表示結果にて、Discards カウンターが 8 ずつ増加します。

○ オートリカバリーが成功したにもかかわらず、リカバリー後に正しく通信できない場合は、代替機の接続先が交換前と同じポートかどうかを確認してください。
誤って交換前とは異なるポートに代替機を接続してしまった場合は、オートリカバリーが動作したとしても、交換前とネットワーク構成が異なるため、正しく通信できない可能性がありますのでご注意ください。

○ atmf cleanup コマンドの実行後、再起動時に HSL のエラーログが表示されますが、通信には影響はありません。

○ リブートローリングの失敗によりローカルエリアが孤立した場合、AMF コントローラー上で show atmf area コマンドを実行すると reachable と表示されてしまいます。

○ AMF ネットワーク名を変更すると、システム再起動を推奨するログの出力と共に、ノードの離脱、再加入が発生しますが、全ノードが再加入できないことがあります。AMF ネットワーク名を変更した後は、必ず再起動を行ってください。再加入できないノードに対しては、Telnet などでログインし、再起動を実施してください。

○ AMF ローカルマスターが VCS メンバーでもある構成において、ローカルマスターをリブートローリングにより再起動すると、AMF コントローラーから当該エリアに対する atmf select-area コマンドの実行に失敗します。ローカルマスターで、エリアリンクまたはバーチャルエリアリンクの設定を行い、直接コアエリアに接続してください。

○ AMF エリアリンクを物理ポートによる接続から、仮想エリアリンクに動的に変更した場合は、ローカルマスターを再起動してください。

○ show atmf detail を実行した際、ドメインの IP 情報が誤って表示されます。

6 マニュアルの補足・誤記訂正

各種ドキュメントの補足事項および誤記訂正です。

6.1 サポートする SFP/SFP+ モジュールについて

本製品がサポートする SFP/SFP+ モジュールの最新情報については、弊社ホームページをご覧ください。

7　サポートリミット一覧

パフォーマンス	
VLAN 登録数	4094
MAC アドレス（FDB）登録数 ※1	16K
IPv4 ホスト（ARP）登録数 ※1	-
IPv4 ルート登録数	-
リンクアグリゲーション	
グループ数（筐体あたり）	18 ※2※3
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
登録数	118 ※4※5※6
認証端末数	
認証端末数（ポートあたり）	1K
認証端末数（装置あたり）	1K
マルチプルダイナミック VLAN（ポートあたり）	1K
マルチプルダイナミック VLAN（装置あたり）	1K
ローカル RADIUS サーバー	
ユーザー登録数	3
RADIUS クライアント（NAS）登録数	1 ※7
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	-

※　表中では、K=1024
※1　システム内部で使用する値を含みます。
※2　AT-x230-18GP の場合。AT-x230-10GP は 10 グループをサポートします。
※3　スタティックチャンネル、LACP 合わせて 18 グループをサポートします。
※4　アクセスリストのエントリー数を示します。
※5　1 ポートにのみ設定した場合の最大数。エントリーの消費量はルール数やポート数に依存します。
※6　ユーザー設定とは別に、アクセスリストを使用する機能を有効化した場合に消費されるエントリーを含みます。
※7　radius-server local コマンドでローカル RADIUS を有効にした際に、自動登録されるローカルホスト（127.0.0.1）を含みます。
ローカルホスト以外の RADIUS クライアント（NAS）を登録したい場合は、no nas 127.0.0.1 コマンドでローカルホストを削除することで登録可能です。

8　未サポート機能（コマンド）

最新のコマンドリファレンスに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

9　最新マニュアルについて

最新の取扱説明書「CentreCOM x230 シリーズ 取扱説明書」(613-001870 Rev.B)、コマンドリファレンス「CentreCOM x230 シリーズ コマンドリファレンス」(613-001990 Rev.C)は弊社ホームページに掲載されています。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/